Todd Whitford

07/27/2011

CI 513

Tech Activity

Internet Safety

1. Based on the information provided in the websites what **Internet safety rules** would you teach upper elementary and middle school students? Consider issues of privacy, safety from predators, inappropriate content, and digital etiquette.

The most important thing for children in this age group to know is how to protect themselves. Elementary and middle school students usually find themselves in trouble online because of mistakes. It is important to have rules to protect their identities. That means never giving out personal information, ensuring privacy settings on social networking sites are set to their highest protection, and never agreeing to meet someone in person that they met online. The reality is that this age group should not be meeting people online at all. Social networking sites like facebook have age requirements for members, but they are easily bypassed. Students in this age group need to have an open line of communication with a responsible adult that they can come to if they see something disturbing online. There is a lot of content online that elementary and middle school students are not ready to be exposed to. They need to have someone that they can go to and speak honestly about any disturbing content they happen upon. As an educator, it is vital that Internet safety information does not end at the classroom door. Parents and guardians need to know how to keep their children safe online as well. Another valuable lesson for students in this age group to know is how to behave when online. They need to know that they are responsible for the information that they seek out and that they will be held accountable if they are engaging in risky online behavior.

2. Based on the information provided in the websites what safety procedures would you teach older students about **social networking**? Consider issues of privacy, inappropriate content, safety, and digital etiquette.

I touched on some of this in my previous response, but to further expand on it I think privacy is the key. The unfortunate reality is that young people are at the most risk when they are engaged in social networking. Older students need to know that what they do online has consequences. Do not put too much personal information online, and protect the information that you do by limiting your privacy settings and not “friending” people you do not know. The Internet should not be a place to meet people; rather it should be used to interact with people you already know. Additionally, social networking opens you up to the realities of cyberbullying. Cyberbullying is a very real problem that exposes students to attacks that can have very real emotional and physical consequences. They also need to be aware that what is online is forever. That negative comment or inappropriate picture or cyberbullying can be spread without individual approval, opening up a Pandora’s box of consequences.

3. Based on the information provided in the websites what safety procedures would you teach middle and high school students about **cyber bullying**? Include the definition of cyber bullying, how to prevent bullying, and what the victim should do.

Cyberbullying is described simply as bullying or harassment that occurs online. Cyberbullying occurs every time the Internet is used to tease, humiliate, or harass someone. While it is generally referred to in terms of social networking sites, it is important to recognize that cyberbullying can also take the form of text messages. Cyberbullying can look like joking around, but the realities of cyberbullying are much more consequential. Cyberbullying can have detrimental emotional and physical repercussions. Students also need to know that cyberbullying is illegal! There are very real legal consequences for engaging in this type of behavior. If a student is a victim of cyberbullying he or she needs to tell someone, not respond to it, and save evidence. If it is having an emotional or physical effect, they need to be encouraged to disengage from the medium (social networking or cell phone) that the bullying is coming from. In this day and age many teachers and administrators are trained in dealing with cyberbullying. They are an invaluable source of conflict resolution that can save lives.  
4. Based on the information provided in the websites what safety procedures would you teach older students about **sexting**? Consider the definition of sexting, possible consequences for the person who sends sexual messages, and how to report sexually inappropriate content.

Sexting is the transmission of sexual content or sexually suggestive content via text message. It can be in the form of text, pictures, or video. The most important thing that students need to know about sexting is that it is illegal and has consequences that can last a lifetime. It is illegal to transmit, receive, share, or have anything to do with the sexualization of minors. It is illegal for anyone to posses a sexual image of a minor, even if that person is your boyfriend or girlfriend. Any nude picture received should immediately be reported to a trusted adult who can then contact the authorities. Sexting can land you in jail, and a conviction will make you a sexual offender who is required to register with the authorities every time you move. The best way to avoid sexting is to maintain a healthy and open relationship with the student. If the student knows the consequences surrounding sexting, they will be more inclined to report the behavior.  
5. Based on the information provided in the websites what safety procedures would you teach middle and high school students about **cyber security**? Consider the dangers from hackers, viruses, and spyware and precautions students can take to avoid these dangers.

Cybersecurity is a serious issue for students, especially when they are using school property to access the Internet. If they are not careful students can fall victim to viruses, phishing, spyware, Trojans, and pharming. The most important thing for students to know is to not access any site unless they can trust it. They need to have clear parameters regarding what a trusted site is and how trusted sites can mean two different things depending on whether a student is doing online research or just surfing the web. The 5 basic cybersecurity tips I found online to protect your computer and identity are to install a firewall to protect the computer from hackers, do not open emails from people you do not know, guard your passwords and do not share them online, type in the website rather than clicking on links, and look for the “https” in the URL window.